

Writing Assignment: Job Analysis
GDIT: Information Security Analyst Principal Position

Troy Bannister

Old Dominion University

IDS 493: Electronic Portfolio Project

Dr. Sherron Gordan-Phan

July 19, 2026

Job Analysis: Information Security Analyst Principal

Abstract

This paper analyzes General Dynamics Information Technology's advertisement for an Information Security Analyst Principal supporting the US Battlefield Information Collection and Exploitation System eXtended program at Langley Air Force Base. The posting describes a senior cybersecurity and information assurance role involving vulnerability assessment, Risk Management Framework (RMF) activities, accreditation maintenance, technical documentation, and communication with government stakeholders. A close reading shows that the employer is looking for someone with more than a basic understanding of Information Assurance tools. The position also requires judgment, prioritization, leadership, and the ability to translate technical findings into operational risk decisions. My cybersecurity coursework, active Secret clearance, Security+ certification, Department of Defense experience, systems administration responsibilities, and exposure to STIG-based compliance provide a relevant foundation. However, the posting and my July 8, 2026, interview also identify development areas, including direct experience with ACAS, SCAP, Splunk, POA&M management, and principal-level RMF responsibilities. The role therefore represents both a credible career target and a practical roadmap for my transition from secure systems administration into formal information assurance and cybersecurity risk leadership.

GDIT: Information Security Analyst Principal Position

The General Dynamics Information Technology (GDIT) advertisement for an Information Security Analyst Principal at Langley Air Force Base represents the type of cybersecurity role I am working toward as I complete my undergraduate degree and continue developing experience in secure Department of Defense (DoD) environments. I applied for the position and interviewed for it on July 8, 2026, which allowed me to compare the written advertisement with the priorities emphasized during the screening process. The posting presents the position as a bridge between technical security operations and formal cyber-risk governance. It requires vulnerability-management and Risk Management Framework (RMF) knowledge, but it also depends on communication, leadership, documentation, and judgment. This analysis argues that principal-level defense cybersecurity requires an integrated combination of technical expertise, compliance fluency, operational awareness, and professional communication; my DoD systems administration experience and cybersecurity education provide a relevant foundation, while the advertisement also reveals the specialized tools and formal information assurance responsibilities I must continue to develop.

Harper (2012) explains that job advertisements can identify workplace expectations, but they still offer a “segmented and partial view of reality” (p. 31). An advertisement presents the employer’s ideal candidate rather than every pressure the employee will experience. My interview provided limited complementary evidence. The recruiter focused on clearance status, certification, examples of professional judgment, and the ability to explain RMF. This verified to me that RMF was not included as decorative or a compliance legalese keyword. GDIT expected applicants to understand it as an operational process and communicate that understanding clearly.

Company, Program, and Position Purpose

GDIT provides technology and mission services to federal, defense, and intelligence customers. This position supports the US Battlefield Information Collection and Exploitation System eXtended (US BICES-X), an internationally distributed program that enables intelligence sharing for military and coalition missions. The employee coordinates with GDIT personnel, the U.S. Air Force, and other government organizations; audits policies and systems; supports inspections; maintains accreditation documentation; evaluates firewall changes; and reports the security posture of classified and interconnected networks (General Dynamics Information Technology [GDIT], 2026). The title *Principal* signals a senior level of independence. The posting calls for ten or more years of related experience, an active Secret clearance, eligibility for a Top Secret/Sensitive Compartmented Information clearance, and the ability to lead less-experienced staff. These requirements suggest that the ideal candidate must interpret findings, defend recommendations, and work credibly with senior government stakeholders rather than wait for detailed instructions.

Technical Requirements and Implied Skills

The most visible technical requirements are ACAS, DISA STIGs, RMF, and Splunk. The responsibilities expand that list to include DISA SCAP, ESS Policy Auditor, POA&M management, vulnerability assessments, security-control validation, and compliance audits across Linux, Windows, Cisco, Juniper, and VMware environments (GDIT, 2026). Their placement in the responsibility section shows that these tools are central to the position. The repeated focus on the “overall program security posture” also makes the scope broader than finding individual weaknesses (GDIT, 2026, “Responsibilities” section). The analyst must determine a finding’s significance, identify a mitigation, document unresolved risk, track

Job Analysis: Information Security Analyst Principal

corrective action, and explain the issue to decision-makers. The National Institute of Standards and Technology (2018) describes RMF as a system life-cycle process connecting control implementation and assessment to authorization and continuous monitoring. The advertisement reflects that same cycle by linking audits, POA&Ms, documentation, risk decisions, and ongoing monitoring.

The posting explicitly seeks a “creative and driven professional” who can work on a “cross-functional, fast paced team” (GDIT, 2026, “Job Description” section). Communication is therefore one of the most important implied skills. The employee must brief senior GDIT and government personnel and translate technical evidence into statements about mission impact, urgency, and accepted risk. Prioritization is equally important because the preferred candidate can “set priorities on multiple projects/tasks at once” (GDIT, 2026, “Preferred Qualifications” section). Vulnerability findings, inspections, documentation deadlines, firewall requests, system availability, and customer demands may all compete for attention. Harris and Clayton (2018) point out that employability skills are used holistically rather than as isolated traits. This job illustrates that point: ACAS knowledge is less useful without interpretation and communication, while RMF knowledge is incomplete without coordination, writing, and evidence management.

Culture, Motivation, and Industry Demand

GDIT’s broader culture materials emphasize connection, knowledge sharing, ethical conduct, honesty, transparency, alignment, and trust (GDIT, n.d.). The job advertisement reinforces a mission-focused and accountable culture. Its invitation to “Own your opportunity” frames the work as personally meaningful and encourages applicants to see themselves as responsible for mission outcomes (GDIT, 2026, “Your Impact” section). The salary range of \$108,800 to \$147,200 and the possibility of obtaining a TS/SCI clearance add practical

Job Analysis: Information Security Analyst Principal

incentives. At the same time, the onsite requirement, classified systems, inspections, and senior reporting imply a controlled and demanding environment. That combination appeals to applicants who value structure, mission, and responsibility, although it may be less attractive to someone seeking remote flexibility or a casual workplace.

The position also reflects a larger shift toward knowledge-based and technology-driven work. Atkinson (2007) argues that modern economic success increasingly depends on knowledge, innovation, technology, and continual skill development. Cybersecurity fits that pattern because tools and standards change while broader abilities in analysis, communication, and judgment remain valuable. The Bureau of Labor Statistics (2025) projects employment of information security analysts to grow 29% from 2024 through 2034, much faster than the average for all occupations. Defense programs create additional demand because systems must remain operational while also meeting formal authorization, documentation, and inspection requirements.

My Preparation and Development Gaps

My coursework and professional experience align with several parts of the posting. CYSE 270, Linux System for Cybersecurity, supports my administration of Red Hat Linux systems through the command line. CYSE 280 strengthened my understanding of Windows administration, access control, and hardening. IT 315 and CYSE 301 developed my networking, security operations, and troubleshooting foundation. CYSE 465, Enterprise Information Assurance for Cybersecurity, connects directly to controls, documentation, compliance, and enterprise risk. CYSE 406 and CYSE 425W also helped me understand that security decisions operate within legal, organizational, and mission requirements. Through CYSE 368, I examined my current work through an academic cybersecurity lens.

Job Analysis: Information Security Analyst Principal

As an LVC Engineering Technician V with systems administration responsibilities, I support Linux/RHEL and Windows systems in a cleared Navy and DoD environment. My duties include account and permission management, access-control and firewall-related troubleshooting, PKI token support, technical documentation, and support for STIG and audit preparation. My active Secret clearance and Security+ certification match important baseline requirements, while my work provides transferable familiarity with government procedures, mission tempo, access restrictions, and contractor-customer relationships. Wright et al. (2011) explain that recruiters evaluate more than objective credentials and make judgments about motivation and person-job fit. My broader DoD experience likely helped establish enough fit to reach the interview despite my tool-specific gaps.

Those gaps remain pretty significant though. I have not independently operated ACAS or SCAP as a primary responsibility, administered Splunk, maintained eMASS authorization records, or owned POA&M management. I also do not have ten years of principal-level cybersecurity experience. My background is more accurately described as security-adjacent systems administration in an RMF-governed environment than ownership of a formal authorization program. The interview made that distinction clearer when I was asked to explain the RMF process. Recognizing framework terminology is different from communicating it fluently under pressure. The honest conclusion is not that I already meet every principal-level requirement, but that I possess a relevant foundation and a clear set of next skills to develop.

Future Challenges and Conclusion

A major challenge in this position would be balancing security enforcement with mission needs. Firewall changes, remediation actions, and control requirements can affect system availability or operational schedules. The analyst must explain why a control matters, what risk

Job Analysis: Information Security Analyst Principal

remains, and which mitigation is realistic. Another challenge would be maintaining accurate evidence across multiple classified systems while responding to changing threats and program priorities. These pressures make the position demanding, but they also explain its appeal. The role moves beyond maintaining systems and toward influencing how technical evidence becomes an organizational risk decision.

Overall, the GDIT advertisement shows that senior defense cybersecurity cannot be reduced to a list of tools. ACAS, SCAP, STIGs, Splunk, POA&Ms, and RMF operate within a larger system of documentation, communication, leadership, and mission accountability. My DoD experience, clearance, certification, coursework, systems administration, and STIG exposure make the position a credible career target, while my limited experience with formal vulnerability-management platforms and authorization artifacts remains a real gap. For that reason, the advertisement and July 8 interview were useful beyond the immediate application. They clarified how my current experience connects to information assurance and provided a practical roadmap for moving from secure systems support into RMF, cyber risk, and future security leadership.

References

- Atkinson, R. D., Information Technology and Innovation Foundation, & Ewing Marion Kauffman Foundation. (2007). Measuring up. In *Economic Development Journal* (Vol. 6, Issue 4, pp. 5–6) [Journal-article].
- General Dynamics Information Technology. (n.d.). *Our culture*. Retrieved July 19, 2026, from <https://www.gdit.com/careers/culture/>
- General Dynamics Information Technology. (2026). *Info. security analyst principal (RQ222538)* [Job advertisement]. <https://www.gdit.com/careers/job/d560c6554/info-security-analyst-principal/>
- Harper, R. (2012). The collection and analysis of job advertisements: A review of research methodology. *Library and Information Research*, 36(112), 29–54.
- Harris, R., & Clayton, B. (2018). Editorial: The importance of skills—but which skills? *International Journal of Training Research*, 16(3), 195–199.
<https://doi.org/10.1080/14480220.2018.1576330>
- Information Security Analysts*. (2025, August 28). Bureau of Labor Statistics.
<https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm>
- National Institute of Standards and Technology. (2018). *Risk management framework for information systems and organizations: A system life cycle approach for security and privacy* (NIST Special Publication 800-37, Revision 2).
<https://doi.org/10.6028/NIST.SP.800-37r2>

Job Analysis: Information Security Analyst Principal

Wright, E. W., Domagalski, T. A., & Collins, R. (2011). Improving employee selection with a revised resume format. *Business Communication Quarterly*, 74(3), 272–286.

<https://doi.org/10.1177/1080569911413809>